ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Prevención de la Ciberdelincuencia y Seguridad Digital del Ciudadano: Estafas, Acoso en Línea y Primera Orientación a Víctimas

6 ECTS | 150 horas | Online, a tu ritmo

Formación acreditada por
Universidad de Vitoria-Gasteiz EUNEIZ



Acerca de ICUFOR

ICUFOR es un centro privado de formación online, Centro Acreditado y Autorizado por la Universidad EUNEIZ de Vitoria-Gasteiz. Diseñamos e impartimos Cursos de Formación Permanente universitarios, pensados para la actualización y la especialización de profesionales en activo.

Nuestros cursos se estudian a tu ritmo en un campus virtual propio y terminan con el diploma de la Universidad EUNEIZ y con certificados de ICUFOR verificables.

Centro acreditado
Universidad EUNEIZ

100 % online
Campus virtual propio

Equipo docente
Disponible todo el curso



Metodología de estudio

Campus virtual propio
Estudias desde cualquier lugar y dispositivo, sin horarios.

Aprendizaje autónomo, pero acompañado
Tú marcas el ritmo y nuestro equipo de docentes resuelve tus dudas y orienta tu estudio.

Contenido del curso en PDF
El material principal, para estudiarlo a fondo, tema a tema.

Abstract de cada tema
Su síntesis, para situarte al empezar y repasar al final.

Presentación con los aspectos clave
Lo esencial de cada bloque, para jerarquizar y fijar.

Cuestionarios de evaluación
De respuesta múltiple, uno por tema.



Campus virtual

Mis cursos
Tu progreso y el siguiente tema por estudiar

Materiales
Contenido en PDF, Abstract y presentación con los aspectos clave

Cuestionarios de evaluación
Tu nota y la revisión de tus respuestas

Equipo docente
Consulta por escrito, chat y asesor de IA a cualquier hora

Secretaría
Certificados en PDF con código de verificación

Pagos y facturas
Descarga de facturas en PDF



Presentación del programa



Amplía tu formación con el Curso de Formación Permanente en Prevención de la Ciberdelincuencia y Seguridad Digital del Ciudadano: Estafas, Acoso en Línea y Primera Orientación a Víctimas, diseñado por ICUFOR para capacitar a profesionales capaces de responder a los desafíos que plantea el entorno digital actual. La creciente sofisticación de las amenazas en línea exige especialistas preparados para identificar riesgos, proteger a la ciudadanía y acompañar a las víctimas de manera integral y eficaz.

Duración
150 horas

Créditos
6 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Analizar los fundamentos, la evolución y la magnitud de la ciberdelincuencia, identificando los perfiles delictivos, las motivaciones y el impacto del fenómeno en la ciudadanía.

Clasificar las principales tipologías de estafas en línea y las técnicas avanzadas de fraude digital emergentes, distinguiendo sus mecanismos de ejecución, señales de alerta e indicadores de detección.

Diseñar estrategias de prevención y autoprotección digital adaptadas al perfil del usuario, aplicando principios de higiene digital, gestión segura de credenciales, protección de dispositivos y mediación parental activa.

Conocer el marco jurídico y normativo aplicable a la ciberdelincuencia, diferenciando la legislación penal española, la normativa europea e internacional y los mecanismos de tutela de los derechos digitales del ciudadano.

Comprender las dinámicas del acoso en línea y sus manifestaciones en poblaciones vulnerables, identificando los factores de riesgo, los perfiles de víctimas y agresores y las consecuencias psicológicas, sociales y legales asociadas.

Dominar los procedimientos de detección de incidentes, preservación de evidencias digitales y formalización de denuncias, utilizando protocolos de respuesta inmediata que garanticen la integridad probatoria y la eficacia del proceso.

Objetivos del curso

Desarrollar competencias de primera orientación y atención integral a víctimas de ciberdelincuencia, aplicando técnicas de escucha activa, evaluación de necesidades y acompañamiento en la recuperación del control digital conforme al principio de no revictimización.

Identificar los recursos institucionales, las redes de cooperación interprofesional y las tendencias emergentes en ciberdelincuencia, relacionando el papel de los organismos de referencia con el diseño de acciones de concienciación ciudadana y la anticipación de nuevos escenarios de riesgo.

Temario

01 Fundamentos de la ciberdelincuencia y el entorno digital contemporáneo

1.1. Concepto y delimitación de la ciberdelincuencia en el contexto tecnológico actual
1.2. Evolución histórica de la delincuencia en el entorno digital
1.3. Perfil del ciberdelincuente: motivaciones, tipologías y modus operandi
1.4. El ecosistema digital como escenario del delito: redes sociales, comercio electrónico y comunicaciones
1.5. Magnitud del fenómeno e impacto de la ciberdelincuencia en la ciudadanía

02 Marco jurídico y normativo aplicable a la ciberdelincuencia y la protección digital del ciudadano

2.1. Legislación penal española en materia de delitos informáticos y ciberdelincuencia
2.2. Normativa europea e internacional sobre ciberdelincuencia y ciberseguridad
2.3. Régimen jurídico de protección de datos personales y su relación con la prevención de ciberdelitos
2.4. Derechos digitales del ciudadano y mecanismos de tutela jurídica
2.5. Responsabilidad legal de plataformas digitales y proveedores de servicios de internet
2.6. Jurisdicción y competencia en delitos cometidos en el ciberespacio

Temario

03 Tipología y mecanismos de las estafas en línea dirigidas al ciudadano

3.1. Clasificación general de las estafas digitales según su naturaleza, canal y objetivo
3.2. Phishing, smishing y vishing: técnicas de suplantación de identidad institucional y corporativa
3.3. Fraudes en comercio electrónico y plataformas de compraventa entre particulares
3.4. Estafas relacionadas con inversiones, criptomonedas y productos financieros fraudulentos
3.5. Fraudes sentimentales y estafas de confianza en plataformas de relaciones interpersonales
3.6. Estafas de falso soporte técnico y distribución de software malicioso
3.7. Fraudes vinculados a ofertas de empleo ficticio y oportunidades laborales falsas

Temario

04 Técnicas avanzadas de fraude digital y nuevas modalidades delictivas emergentes

4.1. Uso de inteligencia artificial en la comisión de estafas y fraudes digitales
4.2. Ataques de ransomware dirigidos a particulares y pequeñas organizaciones
4.3. SIM swapping y secuestro de cuentas digitales: mecanismos técnicos y consecuencias
4.4. Estafas mediante códigos QR fraudulentos y técnicas de quishing
4.5. Fraudes en aplicaciones móviles y riesgos de las tiendas de aplicaciones no oficiales
4.6. La dark web y los mercados ilegales como infraestructura de soporte al fraude digital

05 Acoso en línea: conceptualización, tipología y dinámicas de victimización

5.1. Definición y delimitación conceptual del acoso en el entorno digital
5.2. Tipologías de acoso en línea: cyberbullying, cyberstalking y ciberacoso sexual
5.3. Dinámicas de poder, control y anonimato en las relaciones de acoso digital
5.4. Perfil del acosador en línea: factores de riesgo y patrones de comportamiento recurrentes
5.5. Consecuencias psicológicas, sociales y legales del acoso en línea para las víctimas
5.6. Indicadores de detección temprana de situaciones de acoso digital activo

Temario

06 Ciberacoso en poblaciones vulnerables: menores, personas mayores y colectivos en situación de especial riesgo

6.1. Menores y adolescentes como víctimas de ciberacoso y explotación en línea
6.2. Personas mayores como colectivo especialmente vulnerable ante la ciberdelincuencia
6.3. Violencia digital de género y su intersección con la violencia machista
6.4. Colectivos LGTBI+ y personas con discapacidad ante el ciberacoso y los discursos de odio en línea
6.5. Personas en situación de exclusión social y vulnerabilidad socioeconómica en el entorno digital
6.6. Marco de protección jurídica reforzada para víctimas en situación de especial vulnerabilidad
6.7. Estrategias diferenciadas de prevención y protección adaptadas a cada colectivo vulnerable

Temario

07 Seguridad digital del ciudadano: estrategias de prevención y autoprotección en el entorno conectado

7.1. Principios fundamentales de higiene digital y ciberseguridad personal
7.2. Gestión segura de contraseñas y sistemas de autenticación multifactor
7.3. Protección de dispositivos: actualizaciones de seguridad, software antivirus y configuración avanzada
7.4. Navegación segura y protección de la privacidad en internet
7.5. Seguridad en redes sociales: configuración de perfiles y gestión de la huella digital
7.6. Seguridad en transacciones económicas, banca en línea y medios de pago digitales
7.7. Protección de menores en el entorno digital: controles parentales, mediación activa y comunicación familiar
7.8. Diseño de un plan personal de seguridad digital adaptado al perfil del usuario

Temario

08 Detección de incidentes, preservación de evidencias digitales y procedimiento de denuncia

8.1. Identificación y clasificación de incidentes de ciberdelincuencia sufridos por el ciudadano
8.2. Primeras actuaciones ante la detección de un ciberdelito: protocolo de respuesta inmediata
8.3. Preservación y documentación de evidencias digitales por parte de la víctima
8.4. Proceso de denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado
8.5. Comunicación de incidentes a organismos especializados: INCIBE, AEPD y entidades sectoriales
8.6. El papel del profesional como facilitador y orientador en el proceso de denuncia

Temario

09 Primera orientación y atención integral a víctimas de ciberdelincuencia

9.1. Principios rectores de la atención a víctimas de delitos cometidos en el entorno digital
9.2. Evaluación inicial de las necesidades de la víctima de ciberdelincuencia
9.3. Técnicas de comunicación y escucha activa aplicadas a la atención a víctimas de ciberdelitos
9.4. Orientación sobre derechos reconocidos a las víctimas y derivación a servicios jurídicos, psicológicos y sociales especializados
9.5. Acompañamiento en la recuperación del control digital y la seguridad de la víctima
9.6. Consideraciones específicas en la intervención con víctimas menores de edad y sus familias
9.7. Autocuidado profesional y prevención del desgaste emocional en la atención continuada a víctimas

Temario

10 Recursos institucionales, cooperación interprofesional y tendencias emergentes en la lucha contra la ciberdelincuencia

10.1. Organismos públicos y entidades de referencia en ciberseguridad ciudadana
10.2. Cooperación interprofesional en la prevención y respuesta coordinada a la ciberdelincuencia
10.3. Programas de educación y concienciación ciudadana en seguridad digital
10.4. Tendencias emergentes en ciberdelincuencia y principales desafíos futuros

Titulación y certificados

Diploma de la Universidad EUNEIZ

Al aprobar todos los cuestionarios de evaluación recibes el **diploma en formato digital** de Curso de Formación Permanente, con sus 6 créditos ECTS y 150 horas.

Certificados de ICUFOR

Se descargan en PDF desde la Secretaría del campus, con un código único y QR para verificarlos.



Universidad de Vitoria-Gasteiz EUNEIZ

Proceso de matriculación

1 **Pulsa «Matricularme» en la ficha del curso**
Completa tus datos personales y de facturación.

2 **Elige la forma de pago**
Tarjeta, PayPal o transferencia bancaria.

3 **Entra en el campus y empieza**
Recibes por correo tus datos de acceso y, en cuanto se confirma el pago, tienes el temario completo. La matrícula está abierta todo el año.

Matricúlate | Más información



Métodos de pago

Pago único
El precio se abona una sola vez, sin cuotas ni renovaciones.

Seguridad
Pago online en la pasarela de Stripe o de PayPal.

Flexibilidad
Tarjeta de crédito o débito, PayPal o transferencia.

Acceso inmediato
Con tarjeta o PayPal, el campus se activa al momento.

Simplicidad
Matrícula y pago en dos pasos.

Facturación
Facturas en «Pagos y facturas» del campus.



¿Por qué elegir ICUFOR?

01

Formación accesible

Formación universitaria rigurosa y acreditada, íntegramente online y compatible con tu trabajo.

02

Calidad universitaria

Cada curso está acreditado por la Universidad EUNEIZ, con su memoria académica y sus créditos ECTS.

03

Impulso a tu carrera

Contenidos de utilidad práctica y una titulación que suma en méritos, concursos y bolsas de empleo.

04

Especialización

Cada curso trata una única temática a fondo: combínalos y construye tu propio itinerario.

05

Atención de calidad

Consultas al equipo docente por escrito o por chat, y un asesor de IA a cualquier hora.

¿Por qué elegir ICUFOR?

06

Contenidos actualizados

Los cursos se revisan periódicamente para incorporar las novedades de cada ámbito.

07

El curso, por escrito

Cada tema en tres formatos: contenido en PDF, Abstract y presentación con los aspectos clave.

08

Autónomo, pero acompañado

Tú decides tu ritmo y nuestro equipo de docentes resuelve tus dudas y orienta tu estudio.

09

Enseñanza adaptada

Sin horarios ni conexiones obligatorias: seis meses para terminar, ampliables si lo necesitas.

10

Estudio sencillo e intuitivo

Un campus virtual propio, sin instalar nada y accesible desde cualquier dispositivo.

¿Necesitas más información?

Te contamos cómo funciona el curso, los plazos y la titulación, sin compromiso.

www.icufor.com

info@icufor.com

+34 858 895 080

+34 746 044 519

Formación acreditada por Universidad de Vitoria-Gasteiz EUNEIZ

